ESMA_QA_2219

Submission Date
13/06/2024

Status: Answer Published

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT risk management

Additional Legal Reference
Final Report on Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework

Subject Matter
Questions on Microenterprises and RMF

Question

QUESTION 1: Internal Audit Frequency for Microenterprises and financial entities subject to the simplified risk management framework
Recital 43 of DORA states that microenterprises and financial entities (FEs) referred to in Article 16(1) of DORA are not required to conduct regular internal audits of their ICT risk management framework (RMF). Does it conflict with Article 28, paragraph 5 of Commission Delegated Regulation (EU) 2024/1774 (RTS) that mandates an internal audit on the ICT RMF in line with the FE's audit plan?

QUESTION 2: ICT Testing Requirements for Microenterprises and Financial Entities – Cyber-attack scenarios
Article 11.6 of DORA excludes microenterprises from the requirement to include cyber-attack scenarios in their ICT business continuity and recovery plan testing. Does it conflict with Article 39, paragraph 1 of the Commission Delegated Regulation (EU) 2024/1774 (RTS), which mandates the inclusion of cyber-attack scenarios in the testing plans for financial entities referred to in Article 16(1) of DORA?

QUESTION 3: Recital 43 of DORA specifies that microenterprises and financial entities referred to in Article 16(1) of DORA are not required to regularly conduct risk analyses on legacy ICT systems. Does it conflict with Article 34, paragraph 1, point (e) of the Commission Delegated Regulation (EU) 2024/1774 (RTS) which mandates that financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 must manage the risks related to outdated or unsupported and legacy ICT assets?

ESMA Answer

11-12-2024

Original language

ANSWER 1: Recital 43 does not conflict with Article 28, paragraph 5 of the RTS. The text of Recital 43 in DORA suggests that microenterprises and FEs referred to in Article 16(1) of DORA are not obligated to conduct internal audits of their ICT RMF on a regular basis. This means there is no mandate for these entities to perform the said internal audit with a specific periodicity. However, it does not exclude the necessity of conducting internal audits as deemed necessary by the FE's audit plan. The responsibility for determining the appropriate

frequency and triggers for audits lies with the FE.

ANSWER 2: There is no contradiction between Article 11.6 of DORA and Article 39, paragraph 1 of the RTS. Article 11.6 of DORA explicitly excludes microenterprises from the requirement to include cyber-attack scenarios in their ICT business continuity and recovery plan testing. This exclusion applies solely to microenterprises and not to financial entities referred to in Article 16(1) of DORA. DORA clearly distinguishes between microenterprises and financial entities referred to in Article 16(1) of DORA, ensuring that the latter are still required to include cyber-attack scenarios in their testing plans as per Article 39, paragraph 1 of the RTS.

ANSWER 3: There is no contradiction between Recital 43 of DORA and Article 34, paragraph 1, point (e) of the RTS. Recital 43 specifies that microenterprises and financial entities referred to in Article 16(1) of DORA are not required to regularly conduct risk analyses on legacy ICT systems. This means there is no mandate for these entities to perform risk analyses with a specific periodicity. However, it does not imply that the risks associated with legacy systems should not be managed at all. Article 34 does not specify a required frequency for these risk analyses.